WHITE PAPER

Sechs Basisschritte zur OT-Security
10.2021

von Jens Bußjäger (Achtwerk GmbH, www.acht-werk.de) | Dieter Barelmann (VIDEC Data Engineering GmbH, www.videc.de)

Sechs Basisschritte zur OT-Security

Dem Aufruf, die Projekte im Bereich Digitalisierung zu beschleunigen, wurde in den letzten 2 Jahren verstärkt nachgekommen. In der Situation durchaus verständlich. Unter diesem Druck wurde allerdings häufig ein wichtiger Aspekt aus den Augen verloren.

Aus den Erfahrungen unserer Kundenprojekte und mit unseren Partnern der Systemintegration haben wir sechs wichtige Handlungsempfehlungen zusammengestellt, die eine solide Basis für eine wirksame Risikominimierung und eine zuverlässige Cybersicherheit für OT-Umgebung legen.

In allen Projekten zeigte sich, dass diese sechs Schritte eine wichtige Grundlage für den Aufbau der Cybersicherheit nach dem Stand der Technik sind.

Sicherlich sind diese Punkte nicht allumfassend, aber sie beschreiben die Basics - und damit geht es meistens los.

Schritt 1 - Das Bewusstsein bei den Mitarbeitern für die Gefährdungen schärfen

Es ist nicht richtig sichtbar. Es ist raffiniert und komplex. Es ist vorhanden.

Täglich gibt es mehr als 320.000 Varianten (*BSI-Lagebericht) von Schadsoftware, die hochprofessionell in Phishing-Mails verteilt werden, um Passwörter auszuspionieren und ungesicherte Systeme zu finden.

So infizierte Geräte, Management Laptops und Software sind mit den Produktionsanlagen verbunden. Das Hauptaugenmerk der Betriebsverantwortlichen liegt darauf, die Verfügbarkeit der Produktion zu gewährleisten. Es ist notwendig, diese Gefährdungen kennenzulernen, zu beurteilen und Vorbereitungen für den Fall zu treffen, dass diese Gefährdungen eintreten.

Deswegen macht es durchaus Sinn, die Mitarbeiter ebenfalls auf diese Gefahren zu sensibilisieren.

HINWEIS: Je besser die Mitarbeiter geschult sind, desto besser funktioniert die Abwehr.

Schritt 2 - Die Systeme, die kritisch für die Produktion sind, kennen

Was man nicht kennt, lässt sich nicht schützen! Daher beginnen alle Security-Management Programme und Standards mit dem Asset-Register oder vollständigen logischen Netzstrukturplan.

Im Security-Management sind Assets die Werte der Unternehmen. Dazu zählen

- Gebäude
- Personal
- Lager
- Produktionsanlagen

Für die Absicherung der Produktionsanlage sind Assets die Geräte und Systeme der vernetzten Automatisierung. Türen, Tore, Zäune, Brandmelder, Helme oder Kleidung sind sichtbar. Die vielen Steuerungen, HMIs, Sensoren, Motoren, PLC sind "unsichtbar" in der Maschine und Anlage verbaut. Des Weiteren sind auch die PCs im Leitstand oder z.B. der Arbeitsvorbereitung im Office verbunden. Nicht zu vergessen, die Remote-Zugänge der Integratoren und Hersteller. Das Erkennen dieser "riskanten und offenen" Assets ist vielleicht der wesentlichste Schritt für OT-Sicherheit.

Schritt 3 - Netzwerksegmentierung der OT-Umgebung für mehr Kontrolle

Wir kennen Schotten im Schiffbau und Brandmauern bei Gebäuden. Für vernetzte Produktionsanlagen ist es das Air-Gap-Modell, von dem so viele Anlagen als primäres Sicherheitselement abhängig sind. Doch ist die Trennung von Internet, Office-IT und Produktionsanlage kaum noch vorhanden. Auch werden immer mehr IT-Systeme im Zuge von Industrie 4.0 / der Digitalisierung in der Produktion eingeführt.

Um ein sicheres Zusammenspiel von IT- und OT-Infrastruktur zu ermöglichen und die Digitalisierung zu beschleunigen, ist es wichtig, die Anforderungen an die Netzwerksegmentierung zu durchdenken.

Im Notfall ist es besser, eine System-zu-System-Konnektivität in einem Purdue-Modell herzustellen. Das Ziel muss es sein, diese getrennten kontrollierbaren Bereiche, die sich schützen lassen, wieder bestmöglich zu errichten.

Die Lösung hier ist, "Managed Switches" und Firewalls einzusetzen. Zusätzlich sind Kontrollen der ordnungsgemäßen Funktion (vgl. Schritt 4) einzurichten. So entstehen Segmente (Zonen) und Übergänge (Conduits), die die detaillierte Absicherung im Netzwerk erzeugen.

Schritt 4 - Konsequente Bedrohungsüberwachung und Vorfallmanagement

Transparenz ist der entscheidende erste Schritt für ein wirksames Echtzeit-Monitoring von Cyberbedrohungen. Für Unternehmen ist es unverzichtbar zu wissen, welche Geräte und Systeme sich in ihrer Umgebung befinden, wie die Anlagen miteinander verbunden sind und wie die Netzwerksegmentierung eingerichtet ist.

Sobald Sichtbarkeit hergestellt ist, gilt es zu klären, wie das Netzwerk rund um die Uhr lückenlos überwacht werden soll.

Informationsfluss und Alarmierungsszenarien sind dabei wichtige Bausteine in einer Gesamtstrategie.

HINWEIS: Für Kritische Infrastrukturen (KRITIS) ist mit dem ITSiG 2.0 der Einsatz von Angriffserkennungssystemen in der Automatisierung Pflicht!

Schritt 5 - Konnektivität und Zugangskontrollen

Während es für IT-Umgebungen etablierte Praktiken für das Identitäts- und Zugriffsmanagement gibt, besteht im Bereich OT vielerorts Nachholbedarf. Berechtigungsnachweise werden oft gemeinsam, intern und extern genutzt und der Zugriff ist nicht auf bestimmte Netzwerkgeräte oder -segmente beschränkt.

Strategie 6 - Schwachstellen- und Patch-Management

Altsysteme, geschäftskritische Rahmenbedingungen und die begrenzten Patch-Fenster von OT-Umgebungen erschweren es typischerweise, eine ganzheitliche Strategie für das Gefahrenabwehr- und Patch-Management zu entwickeln.

Anstatt sich durch Hunderte von Schwachstellen zu patchen müssen Anwender verstehen, welche potenziell gefährdeten Systeme für die Produktion am wichtigsten sind. Idealerweise werden Sicherheitslücken im Zuge der nächsten regelmäßigen Wartung geschlossen - mit dem Wissen im Hinterkopf, dass für viele OT-Schwachstellen überhaupt kein Patch oder Firmware-Update verfügbar ist.

HINWEIS: Viele der bekannten Software-Schwachstellen der eingesetzten Systeme sind nicht zwingend zu Patchen. Die Maßnahmen der Schritte 1-5 sind oft ausreichend!

Vielen Dank an unsere Partner für den Austausch und die Informationen.

Aktuell freuen wir uns über vier weitere IRMA® System Partner:

INTERNATIONAL

- Demont in der Schweiz | www.demont.swiss

NATIONAL

- Focus Industrieautomation GmbH in Merenberg | www.focus-ia.de
- IAT GmbH in Brandenburg | www.iat-rur.de
- gat GmbH in Schwalbach | www.gatgmbh.de